

## **SECTION C - PERFORMANCE WORK STATEMENT**

### **C.1 INTRODUCTION**

The General Services Administration (GSA) Federal Acquisition Service (FAS) Information Technology Category (ITC) Office of Telecommunications Services (OTS) develops and manages programs that meet the current and future telecommunications requirements of Federal agencies and departments. In addition, the Office of Telecommunications Services delivers administrative and technical support for services and solutions that are both efficient and cost-effective.

The Office of Telecommunications Services accomplishes this by:

Effectively leveraging competition to offer the best available telecommunications services and solutions at the best overall prices in the marketplace and providing a customer focused, highly responsive, and fully integrated approach to helping Federal agencies.

Office of Telecommunications Services programs are available to Federal departments and agencies that meet the eligibility criteria contained in the GSA Directive ADM 4800.2G, Eligibility to Use GSA Sources of Supply and Services, dated September 17, 2009. Telecommunications services include data, voice, and video across a variety of transmission media such as radio, wire, cable, satellite, wireless. IT Security requirements must also be addressed.

The Office of Telecommunications Services currently offers the following technology contracts:

- [Networx \(Universal and Enterprise\)](#)  
Two broadly scoped acquisitions providing comprehensive service suites of telecommunication/IT services (will be replaced by the Enterprise Infrastructure Solutions [EIS] contracts).
- [Future COMSATCOM Commercial Services Acquisition \(FCSA\)](#)  
FCSA was created in partnership with the Department of Defense to create a multi-billion dollar common marketplace for the entire Federal Government to procure its commercial SATCOM services. It encompasses new Special Item Numbers on Federal Supply Schedule 70 and two new multiple-award ID/IQ contract vehicles, Custom SATCOM Solutions (CS2) and CS2-Small Business (CS2 and CS2SB will be replaced by CS3).
- [CONNECTIONS II \(CNX II\)](#)  
CNX III is a \$5 billion, 10-year multiple award contract that will be the Government's one-stop shop for obtaining telecommunications, network and communications solutions.
- [Federal Relay](#)  
Telecommunications access for Federal employees who are deaf, hard of hearing or speech disabled.
- [Telecommunications Expense Management Services \(TEMS\)](#)  
Convenient and single-source for ordering and managing wireless devices and service from regional or local carriers.
- [Local Telecommunications Services Contracts](#)  
Full range of first mile/last mile services and solutions.
- [Enterprise Infrastructure Solutions \(EIS\)](#)  
This acquisition is replacing GSA's current Networx Universal and Enterprise contracts as well as GSA Regional Local Service Agreements for government telecommunications and infrastructure solutions.

The Security Solutions Branch provides professional security services to GSA's internal and external clients with Information Security Officer (ISSO) support for the systems listed in Section C.3.2, personnel security, industrial security, as well as security consultant support to GSA (see Attachment "A" for the Security Solutions Branch Functional Responsibilities Matrix).

## **C.2.0 SCOPE**

The scope of work includes providing the GSA with comprehensive IT technical subject matter expert support to assist the Security Solutions Branch in ensuring contractual compliance with information assurance and IT security requirements and providing ongoing technical refreshment of the contracts listed in Section C.1 and any future acquisition initiatives assuring continued overall security compliance, and performing system security assessment services for the systems identified in Section C.3.3 and any future initiatives ensuring operational compliance.

- Perform all duties associated with an Information System Security Officer (ISSO). Reference Attachment “B”.
- Assist with development, reviews and maintenance of information system assessments and authorization (formerly known as Certification and Accreditation) documentation.
- Provide advice on emerging technologies and associated information assurance requirements.
- Review and provide recommended changes to newly developed/updated government guides, directives, policies and procedures (both Federal and Agency Level) relative to information assurance and security.
- Provide assistance with reviewing and updating contract deliverables associated with information assurance and security.
- Assist with the development of contract information assurance and IT security requirements relative to ITC programs.
- Support may also include attendance at security conferences/forums, technical research and analysis for presentations, white papers, position papers, and to brief the findings relative to information assurance and security.
- Provide independent third-party system security assessment services to include developing associated Security Assessment Reports.
- Perform system scans which include Web, Operating Systems and Database applications.
- Perform on-site inspections and interviews as required.
- Perform penetration tests to include developing associated reports.

## **C.2.1 OBJECTIVES**

The primary objective of the support to be provided under this task order is to ensure a solid, viable Information Assurance (IA) program for the systems that support our Government and Commercial clients. At a minimum our goals are to:

- Ensure accurate, timely, and quality personnel security documentation and processing for internal and external clients;
- Ensure accurate, timely, and professionally prepared industrial security documentation for internal and external clients;
- Ensure quality development, and reviews of all documents associated with systems security;
- Ensure accurate, thorough, and timely analysis of vulnerability scans and associated documentation; and
- Fully support the GSA CIO’s systems security efforts in accordance with all directives, security procedural guides, and standards.

## **C.3.0 TASK REQUIREMENTS**

### **C.3.1 Subtask 1 – Program Management**

The Contractor shall manage the tasks in this PWS in accordance with best practices established by the Program Management Institute (PMI), as described in the current PMI Project Management Body of Knowledge (PMBOK) Guide, and other applicable PMI publications and media. The Contractor shall perform management activities to include risk, quality, schedule, asset, and configuration management. The Contractor shall identify a Program Manager (PM), by name, who shall provide management, direction, administration, quality assurance, and leadership for the execution of this task order. The Contractor shall provide appropriately cleared, certified, trained, and qualified personnel to support contract requirements, as well as all necessary personnel management services that are required to satisfy performance requirements.

#### **C.3.1.1 Subtask 1-1- Coordinate Task Order Kickoff Meeting**

The Contractor shall schedule and coordinate a Task Order Kick-Off Meeting at the location approved by the Government. The meeting will provide an introduction between the Contractor personnel and Government personnel who will be involved with the task order. The meeting will provide the opportunity to discuss technical, management, and IT security issues, and travel authorization and reporting procedures.

#### **C.3.1.2 Subtask 1-2 - Transition-In Plan**

The contractor shall provide a draft Transition-In Plan. The plan shall articulate as needed:

- The Contractor's transition approach, process and timelines.
- The Contractor's approach to mitigating or minimizing disruption.
- The Contractor's staffing status.
- Transition risk management and mitigation strategy
- Initial coordination with the prior Contractor.
- Gap analysis of required skills
- Training approach/knowledge transfer approach.

The Contractor shall execute its Government-approved Transition-in Plan. As part of this plan, the Contractor shall ensure there will be minimum service disruption to vital Government business and no service degradation during and after transition. All transition activities will be completed within 30 calendar days after the Project Kick-Off Meeting.

#### **C.3.1.3 Subtask 1-3 - Prepare Monthly Status Report (MSR)**

The Contractor Program Manager shall develop and provide a MSR using MS Office Suite of applications, by the 10<sup>th</sup> calendar day of each month via electronic mail to the Contracting Officer's Representative (COR). The report shall include the following:

- Activities during the reporting period, by task (Include: On-going activities, new activities, activities completed; progress to date on all above mentioned activities). Start each section with a brief description of the task.
- Problems and corrective actions taken. Also include issues or concerns and proposed resolutions to address them.
- Personnel gains, losses and status (security clearance, etc.).
- Any government actions required.
- Schedule (Shows major tasks, milestones, and deliverables; planned and actual start and completion dates for each).
- Summary of any travel taken, conferences attended, etc. (Attach trip reports to this MSR for reporting period).
- Accumulated invoiced cost for each CLIN up to the previous month.
- Projected cost of each CLIN for the current month.

#### **C.3.1.4 Subtask 1-4 – Convene Technical Status Meetings**

The Contractor Program Manager shall convene a monthly Contract Activity and Status Meeting with the COR, and other key government stakeholders. The purpose of this meeting is to ensure all stakeholders are informed of the monthly activity and status report, provide opportunities to identify other activities and establish priorities, and coordinate resolution of identified problems or opportunities. The Contractor Program Manager shall provide minutes of these meetings, including attendance, issues discussed, decisions made, and action items assigned, to the COR within five (5) calendar days following each meeting.

#### **C.3.1.5 Subtask 1-5 - Prepare Program Management Plan (PMP) For Specific Taskings**

The Contractor shall submit a Program Management Plan (PMP) detailing how all aspects of the IT Services shall be obtained, how each of these activities shall be executed, and the Contractor's specific role in program execution. When required by the COR, the Contractor shall document all support requirements in a PMP for special projects/initiatives undertaken by the Security Solutions Branch that come up during the life-cycle of the task order. The PMP shall:

- Describe the proposed management approach.
- Include milestones, tasks, and subtasks required in this task order.
- Provide for an overall Work Breakdown Structure (WBS) and associated responsibilities and partnerships between Government organizations.
- Include the Contractor's Quality Control Plan (QCP) (if applicable).

The Contractor shall provide the Government with a draft PMP, on which the Government will make comments. The final PMP shall incorporate Government comments.

### **C.3.1.6 Subtask 1- 6 - Prepare Trip Reports**

The Government will identify the need for a Trip Report (if required) when the request for travel is submitted (see Attachment "C"). A trip report will be due within 10 workdays following completion of each trip. The Contractor shall keep a summary of all long-distance travel, to include, at a minimum, the name of the employee, location of travel, duration of trip, and POC at travel location.

### **C.3.2 Subtask 2 - Information Assurance Support**

The Contractor shall provide professional expertise in supporting requirements associated with Information Assurance (IA) and IT security requirements associated with the governments need to meet Federal Information Security Management Act (FISMA) mandates. This support will include but is not limited to reviews of IA and FISMA related security documentation associated with contract deliverables, GSA Security policies and procedures, assisting with Information Systems Security Officer (ISSO) requirements and attending related meetings, seminars and conferences. This support will require expert knowledge of Intelligence Community (IC), Department of Defense (DoD) as well as Federal Civilian Government policies and procedures. The Contractor shall also become thoroughly familiar with information assurance and security related policies and procedures for GSA as well as client agencies. The Security Solutions Branch currently requires IA and FISMA support associated with the following systems: Networkx Universal and Enterprise Contracts Operational Support Systems (OSS) for AT&T, CenturyLink, Level 3, and Verizon; MTIPS systems for AT&T, CenturyLink, and Verizon Business Services; Network Hosting Center (NHC); Conexus; Enterprise Infrastructure Services (EIS) Business Support Systems for AT&T, BT Federal, CenturyLink, Core Technologies, Granite, Harris Corporation, Manhattan Telecommunications (MetTel), MicroTech, and Verizon Business Network Services; EIS MTIPS for AT&T, BT Federal, CenturyLink, Granite, and Verizon Business Network Services, FedRelay, and Commercial Satellite Communications (CS3) contracts.

Support and deliverables associated with task area are:

- a. Provide assistance with creating and modifying Standard Operating Procedures for tasks associated with Security Assessments and Authorizations, continuous monitoring and annual reviews within 10 workdays of assignment by the COR.
- b. Provide assistance in developing and maintaining training plan for internal security staff within 10 workdays of assignment by the COR.
- c. Provide assistance in creating, modifying and maintaining, with 99.999 % accuracy, online dashboards related to the current security posture of and progress of deliverable submission for all systems owned by ITC within five (5) workdays as identified by the COR and maintaining on an on-going basis.

- d. Provide assistance with reviewing monthly/quarterly Plan of Actions & Milestones (POA&Ms) and associated system scans as well as submitting the review results to the GSA/FAS/CIO Security Office. The POA&Ms and scans shall also be posted to the GSA/OCIO/OCISO secure data storage sites (locations to be identified by the COR. Specific due dates for the quarterly POA&M reviews will be provided for each fiscal year as determined by the Chief Information Security Officer (CISO).
- e. Provide assistance with system security assessments/re-assessments and authorizations for Networx OSSs, EIS BSSs, MTIPS, and other GSA systems as necessary to ensure that these systems retain their Authority-To-Operate (ATO). This includes reviewing System Security Plans (SSP) and associated appendices/attachments for accuracy and compliance. Documentation review reports due within five (5) to 10 workdays from receipt of SSP and associated appendices/attachments.
- f. Provide assistance with reviews and approvals of annual Contingency Test Plan Reports (CTPR) for supported systems – Report due within five (5) workdays from receipt of annual report.
- g. Provide assistance with reviews and approvals of annual Incident Response Test Reports (IRTR) for supported systems – Report due within five (5) workdays from receipt of annual report.
- h. Provide assistance with Annual FISMA Reviews and Data Calls for all ITC Office of Telecommunications Services systems to GSA/CIO – date varies dependent upon DHS/OMB requirements but normally occurs during June/July timeframe. Delivery of reviews due within 10 workdays after receipt of completed FISMA Reviews and Data Call documents.
- i. Provide reviews of all newly developed or updates to GSA IT Security Policies and Guides – report due within five (5) workdays after receipt of draft – final due dates determined by GSA/OCIO/OCISO.
- j. Provide assistance with preparation and delivery of final/approved versions of GSA Policies and Guide to appropriate Contractor Security Managers – review due within five (5) workdays after distribution by GSA/OCISO.
- k. Provide assistance with reviewing documentation associated with system modifications that affect system security posture – report due within five (5) workdays after receipt of modification documentation.
- l. Provides assistance with reviewing annual contract deliverables as well as other changes that may affect security posture that are submitted by program managers and system owners/security managers – reports due within five (5) of receipt of changed/updated documents.
- m. Provide assistance with the development of acquisition requirements and associated documentation related to FISMA, Information Assurance and Security within five (5) workdays of receipt of assignment.
- n. Attend NIST Federal Computer Security Program Managers (FCSPM) meetings – specific anticipated dates are provided by NIST each year – February, April, June (Annual Offsite), August, October and December (actual attendance dates posted about one month prior to meeting). A summary is due within five (5) workdays of completion of Meetings, Seminars, and Conferences
- o. Attend Security Conferences to enhance security knowledge and maintain security certifications and qualifications as necessary. A summary report is due within five (5) workdays of completion of Conferences.
- p. Provide Continuous Vulnerability Monitoring services for the systems associated with the Office of Telecommunication Services in accordance with GSA directives and security guides on an on-going basis.
- q. Reviews and provides input, at the government's request, on security-related documentation, or Incident Response reports as identified by the COR within five (5) workdays of assignment.

Note: All deliverables require 99.999 % accuracy.

The deliverables for this subtask are included in Section F.

### **C.3.3 Subtask 3 - Systems Security Assessment Support (As Required)**

The contractor shall provide professional expertise in supporting requirements associated with the performance of system security assessments associated with the governments need to meet Federal Information Security Management Act (FISMA) mandates, all appropriate related government and agency policies, directives, security and hardening guides as well NIST Special Publications. This support will include but is not limited to reviews of

System Security Plans and associated appendices/attachments; performance of database, web application and operating system scans when identified by the government; development of a Security Assessment Report (SAR), POA&M and associated authority to operate recommendation letters. This support will require expert knowledge of the Department of Defense (DoD), Federal Civilian Government, and Intelligence Community (IC) directives, policies, and procedures. The contractor shall also become thoroughly familiar with information assurance and security related policies and procedures for GSA as well as client agencies. The Security Solutions Branch is currently responsible for maintaining the Authorization to Operate for the following systems: Networx Universal and Enterprise Contracts Operational Support Systems (OSS) for AT&T, CenturyLink, Level 3, and Verizon; MTIPS systems for AT&T, CenturyLink, and Verizon Business Services; Network Hosting Center (NHC); Conexus; Enterprise Infrastructure Services (EIS) Business Support Systems for AT&T, BT Federal, CenturyLink, Core Technologies, Granite, Harris Corporation, Manhattan Telecommunications (MetTel), MicroTech, and Verizon Business Network Services; EIS MTIPS for AT&T, BT Federal, CenturyLink, Granite, and Verizon Business Network Services, and FedRelay. The listing of system security ATOs with their expiration dates are in Attachments "A" of this PWS. The number of system security assessments to be performed per month varies as noted in attachment "A", and it is possible that some of these assessments may occur simultaneously.

Support and deliverables associated with task area are:

- a. Set up, coordinate and perform security assessment initiation meeting where initial security assessment documentation will be provided to the third party assessment team. Due within five (5) workdays of receipt of system documentation.
- b. Develop a Security Assessment Plan (SAP) in accordance with GSA CIO IT Security Procedural Guide 06-30, Security Assessment and Authorization, Planning, and Risk Assessment. The SAP is due within ten (10) workdays of initiation meeting.
- c. Develop Rules of Engagement (RoE) for systems to be assessed. Due within five (5) workdays of the initiation meeting.
- d. Upon approval of SAP and RoE, perform security assessment to include scheduling of interviews, system scans as necessary and penetration testing.
- e. Conduct authenticated vulnerability scanning servers' operating systems when identified by GSA.
- f. Conduct authenticated vulnerability scanning of web servers when identified by GSA.
- g. Conduct authenticated vulnerability scanning of database servers when identified by GSA.
- h. Perform assess of security controls following the SAP and using the GSA Assessment Test Cases.
- i. Conduct configuration compliance scanning of all networking devices when identified by GSA. Scan results due within 15 workdays.
- j. Perform internal and external penetration testing to include Penetration Test Report (PTR). PTR is due within five (5) workdays of completion of tests.
- k. Develop a system security assessment Plan of Actions & Milestones (POA&Ms) to include all Critical, High and Moderate vulnerabilities identified during system scans. The POA&M is due within 20 workdays from completion of scans.
- l. Conduct code analysis to examine any developed software for common flaws and document the results in a Code Review Report when identified by GSA. This report will be due within five (5) days after completion of code analysis.
- m. Documentation review reports due within five (5) to 10 workdays of completion of site visits.
- n. Prepare a Security Assessment Report (SAR) documenting the issues, findings, and recommendations of the security control assessment. Document the assessment findings with recommendation(s) and risk determinations from the NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments. Draft SAR

is due within 20 workdays of completion of site visits. Final version will be due within five (5) workdays of receipt of GSA comments.

Note: All deliverables require 99.999 % accuracy.

The deliverables for this subtask are included in Section F.

#### **C.3.4 Subtask 4 - Surge Support (Optional Services)**

Due to the potential of significant increases in security workloads in any of the subtasks identified within this PWS, the contractor may be required to provide additional surge support to handle these additional requirements. All deliverables and performance measures will remain the same as currently identified in sections C.3.2 Subtask 2 - Information Assurance Support and C.3.3 Subtask 3 - Systems Security Assessment Support (As Required).

#### **C.3.5 ASSUMPTIONS**

This section defines the overall assumptions underlying this task which the Contractor should consider in developing their technical solutions to the subtasks in Section C.3:

- The Contractor shall use the available Government Furnished Information (GFI) and, where effective and appropriate, automated tools of the Office of Telecommunications Services (e.g., Networx Hosting Center) to analyze process and store contract sensitive and controlled unclassified information (CUI). Access to all relevant GFI will be provided after award.
- The Contractor shall consider Government requirements for IT security and privacy and their potential impact to service delivery during contract security requirements development processes.
- The Contractor may use any existing tool set made available by GSA or to which they have access in determining, documenting, and supporting their information assurance and IT security analyses.

**END OF SECTION C**